

Copyright and Patent Information

Copyright© 1998 - 2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, Mobile User VPN, and MUVPN are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks and tradenames are the property of their respective owners.

Printed in the United States of America.

Part No: 1200016

WatchGuard® Mobile User VPN End User Brochure—Windows NT

WatchGuard Mobile User VPN creates a secure tunnel between a remote computer and a company network over the Internet. In other words, you can connect to the Internet from home or on the road and then communicate safely and security with your company network to read mail, browse Network Neighborhood, or access shared files.

What do I need?

Every computer used as a MUVPN remote host must have the following system requirements. Further, each platform variation must also be setup properly and be configured to use the remote WINS and DNS servers on the network behind the Firebox.

System Requirements

- PC-compatible computer with Pentium processor or equivalent
- Minimum RAM for Microsoft Windows NT 4.0 Workstation: 32 MB
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Ethernet for network connections
- Microsoft Internet Explorer 4.0 or later
- An Internet Service Provider account
- A Dial-Up or Broadband (DSL or Cable modem) Connection

The Mobile User VPN Adapter, which supports L2TP, installs only if these network components are already installed on your computer:

- Windows NT: Remote Access Server (RAS)

If these components are not installed, follow these instructions:

Installing Remote Access Server on Windows NT

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
- 2 Select the **Services** tab.
- 3 Click the **Add** button.
- 4 Select **Remote Access Services** from the list, then click the **OK** button.
- 5 Enter the path to the Windows NT install files or insert your system installation CD, then click the **OK** button.
The Remote Access Setup dialog box appears.
- 6 Click the **Yes** button to add a RAS capable device and enable you to add a modem.
- 7 Click the **Add** button and complete the Install New Modem wizard

NOTE

If there is no modem installed, you can enable the **Don't detect my modem; I will select it from a list** checkbox then add a Standard 28800 modem.

- 8 Select the modem added in the last step in the Add RAS Device dialog box, then click the **OK** button.
- 9 Click the **Continue** button, then click the **Close** button.
- 10 Reboot your computer.

Configure the WINS and DNS Server Settings

In order for Windows file and print sharing to occur through the MUVPN tunnel, the remote host computer must be configured to use the WINS and DNS servers on the trusted and optional networks behind the Firebox.

from the network before it times out and completes the shut down cycle.

I lost the connection to my ISP, and now I can't use the company network...

If you lose Internet connection long enough, MUVPN also loses the secure tunnel. Follow the steps to close the tunnel. Then connect to the Internet and restart the MUVPN client.

No matter what I do, I can't use the company network...

There may be a problem with the configuration file (.wgx) or shared passwords.

your computer secure from unauthorized incoming or outgoing traffic. Unfortunately, it may block your computer from broadcasting its network information thereby preventing the machine from sending the necessary login information. You should be certain to shut down ZoneAlarm each time you disconnect the MUVPN connection.

Is the Mobile User VPN tunnel is working...

The Mobile User VPN client icon, which appears in the Windows desktop system tray once it has been launched, will display a key within the icon once the client has connected.

To test the connection, ping a computer on your company network.

- Select **Start** ⇒ **Run**. Type `ping` and the IP address of a computer on your company network.

My mapped drives have a red X through them...

The Windows operating system verifies and maps network drives automatically when the computer starts. Because there is no way for you to establish a remote session with the company network before the computer actually starts, drive mapping fails during the boot process and a red X appears on the drive icon. Establish a MUVPN tunnel and open the network drive. The red X should disappear.

I sometimes get prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products only allow access to a single network domain. If your company is large enough to require subnetting (multiple networks connected together), you will only be able to browse your own domain. Attempts to access other domains will result in a password prompt. Unfortunately, even providing the correct information will not open these additional networks.

It takes a *really* long time to shut down the computer after using Mobile User VPN...

If you open and browse a mapped network drive during a MUVPN session, the Windows operating system waits for a signal

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Click the **Protocols** tab.
- 3 Select the **TCP/IP** protocol and click the **Properties** button.
The Microsoft TCP/IP Properties window appears.
- 4 Click the **DNS** tab.
- 5 Click the **Add** button.
- 6 Enter your DNS server IP address in the appropriate.
If you have multiple remote DNS servers repeat the last two steps.

CAUTION

Make certain that your DNS server on the Trusted network behind the Firebox is listed first.

- 7 Click the **WINS Address** tab.
- 8 Enter your WINS server IP address in the appropriate field, then click the **OK** button.
If you have multiple remote WINS servers repeat this step.
- 9 Click the **Close** button to close the Network window.
The Network Settings Change dialog box appears.
- 10 Click the **Yes** button to restart the computer and effect the changes.

Platform Setup

Adding a Domain Name to a Windows NT Workstation

Often remote clients need to connect to a domain behind the firewall. To do this, the remote client must be able to recognize the domains to which they belong. Adding a domain requires the installation of the Computer Browser Network Service.

Installing the Computer Browser

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network dialog box appears.
- 2 Click the **Services** tab.
- 3 Click **Add**.
- 4 Select **Computer Browser**.
- 5 Browse to locate the installation directory. Click **OK**.
- 6 Reboot the workstation.

Adding a New Domain

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network dialog box appears.
- 2 Click the **Protocols** tab.
- 3 Select **Computer Browser**. Click **Properties**.
- 4 Add the remote network domain name.
You can add multiple domain names during the same configuration session.
- 5 Click **OK**.
- 6 Reboot the workstation.

Installation Requirements for Mobile User VPN

To install and run the Mobile User VPN, you must receive the following from your network administrator:

- Software installation package.
The packages are located on the WatchGuard LiveSecurity site at:
www.watchguard.com/support
- Configuration file
A file containing the user name, shared key, and settings that enable a remote computer to connect securely over the

My computer is hung up just after installing the MUVPN client...

This is most likely due to either the ZoneAlarm personal firewall application interfering with regular Local network traffic or the MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm should be shutdown and the client deactivated.

From the Windows desktop system tray:

- 1 First, reboot your computer
- 2 Right-click on the Mobile User VPN Client icon.
- 3 Select **Disconnect All**.
The MUVPN Client closes all VPN tunnels.
- 4 Right-click on the Mobile User VPN Client icon and select **Deactivate Security Policy**.
The MUVPN icon will display a red slash to indicate that the Security Policy has been deactivated.
- 5 Right-click on the ZoneAlarm icon and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 6 Click the **Yes** button when prompted to quit ZoneAlarm.

I have to enter my network log in information even when I'm not connected to the network...

When you start your computer, you are prompted to enter your Windows network user name, password and domain. It is very important that you enter this information correctly, just as you would if you were at the office connected to the network. Windows stores the information for use by network adapters and networked applications. Later, when you connect to your ISP and start the MUVPN client, your computer uses the stored user name, password, and domain to connect to the company network.

I am *not* prompted for my user name and password when I turn my computer on...

This is most likely due to the ZoneAlarm personal firewall application. This program is very good at what it does: keeping

home page. The program which actually needs to pass through the firewall is "IEXPLORE.EXE".

In order to allow this program access each time the application is executed, enable the **Remember the answer each time I use this program** checkbox.

Here is a list of a few essential programs which will need access through the ZoneAlarm personal firewall in order to operate some important applications.

Programs Which *Must* Be Allowed

<i>MUVPN client</i>	IreIKE.exe MuvpnConnect.exe
<i>MUVPN Connection Monitor</i>	CmonApp.exe
<i>MUVPN Log Viewer</i>	ViewLog.exe

Programs Which *May* Be Allowed

<i>MS Outlook</i>	OUTLOOK.exe
<i>MS Internet Explorer 5.x</i>	IEXPLORE.exe
<i>Netscape 6.1</i>	netscp6.exe
<i>Standard Windows network applications</i>	lsass.exe services.exe svchost.exe winlogon.exe

Troubleshooting Tips

WatchGuard maintains a knowledgebase on our Web site, including an In-Depth FAQ section on configuring and using the MUVPN client. This is available at:

www.watchguard.com/support

A few of the most common issues found in installing, configuring, and using the MUVPN client are described below.

Internet to a protected private computer network. The configuration file has the filename: *username.wgx*

- **Shared Key**

In order to install the configuration file, the user is prompted for a shared key. This key decrypts the Mobile User VPN configuration file and imports the security policy into the Mobile User VPN client. It is set during the creation of the .wgx file at the Policy Manager.

Installation

You must install the MUVPN software on your computer. The installation process consists of two steps: installing the MUVPN client and importing the configuration file (.wgx) into the client.

- 1 Copy the software installation package to the Windows desktop.
- 2 Copy the configuration file (.wgx file) to the computer's c:\ directory.
- 3 Double-click the software installation package executable file.
- 4 The installation package welcomes you to the InstallShield Wizard. Click the **Next** button.

NOTE

During the Setup Status portion of the install procedure, the InstallShield may detect ReadOnly Files. If this occurs, click the **Yes** button for each event in order to continue the install.

- 5 The installation package again welcomes you to the InstallShield Wizard. Once more, click the **Next** button. The Software Licence Agreement appears.
- 6 Click the **Yes** button, to accept the terms of the License Agreement and to continue with the installation.
- 7 Select the type of setup, by default Typical is enabled—this is the setup recommended by WatchGuard. Click the **Next** button.
- 8 Keep the default components, click the **Next** button.

- Click the **Next** button to begin copying files.

NOTE

A command prompt window will appear while the `dni_vapmp` file is installed—this is normal. When it is complete, the installation will continue.

- When the InstallShield Wizard is complete, click the **Finish** button.
- The InstallShield Wizard then searches for the `.wgx` configuration file at the computer's root directory, `c: /`. If the file was not copied to this default directory, you must use the **Browse** button to locate and select the proper folder.
- The InstallShield Wizard has completed the install of the MUVPN Client, verify that the option **Yes, I want to restart my computer now** is enabled and click the **Finish** button.

Import the Configuration File

Once you have restarted the machine, the WatchGuard Policy Import dialog box appears. Import the MUVPN configuration file and provide the Shared Key used to decrypt the file.

Once you have restarted the machine, the WatchGuard Policy Import dialog box appears. Import the MUVPN configuration file (`.wgx`) and provide the Shared Key used to decrypt the file.

- The WatchGuard Policy Import window should locate the configuration file (`.wgx`) in the directory specified during the installation.

NOTE

If the WatchGuard Policy Import tool does not locate the `.wgx` file, click the **Browse** button and locate the file.

- Enter the Shared key in the appropriate field. Then click the **OK** button.
- You have finished setting up the Mobile User VPN client. Click **OK**.
The remote host is now ready to use Mobile User VPN.

- Verify that the option **Yes, I want to restart my computer now** is enabled and click **Finish**.
The computer will reboot.

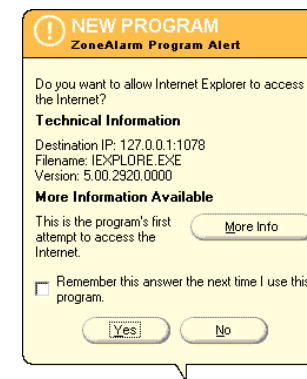
NOTE

The ZoneAlarm personal firewall settings are preserved under the following default directory, `c:\winnt\internet logs\`. If you wish to disregard these settings, delete the contents.

- When the computer has restarted, select **Start ⇒ Programs**.
- Right-click on **Mobile User VPN** and select **Delete** to remove this selection from your Start Menu.

Allowing Traffic through ZoneAlarm

When an application requires access through the ZoneAlarm personal firewall, a Program Alert will be displayed on the Windows desktop informing the user which particular program needs access. Often, the program associated with the application is not readily indicative of the application the user is attempting to execute.



In the example above, the Internet Explorer Web browser application has been launched and is attempting to access the users

If you are using the ZoneAlarm personal firewall, deactivate this as well.

From the Windows desktop system tray:

- 1 Right-click on the ZoneAlarm icon and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

Uninstall the Mobile User VPN Client

At some point, it may become necessary to completely uninstall the MUVPN client. WatchGuard recommends a complete uninstall using the Windows Add/Remove Programs tool.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.
The Control Panel window appears.
- 2 Double click on the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.
- 3 Select **Mobile User VPN** and click on the **Change/Remove** button.
The InstallShield Wizard window appears.
- 4 Select **Remove** and click the **Next** button.
The Confirm File Deletion dialog box appears.
- 5 Click the **OK** button to completely remove all of the components.

NOTE

A command prompt window will appear while the `dni_vapmp` file is uninstalled—this is normal. When it is complete the process will continue.

The Uninstall Security Policy dialog box appears.

- 6 Click the **Yes** button to delete the Security Policy Personal Certificates and Private/Public Keys.
The InstallShield Wizard window appears.

Connection

The MUVPN client enables the remote host computer to establish a secure, encrypted connection to a protected network over the Internet. To do this, you must first connect to the Internet and then use the MUVPN client to connect to the protected network.

- 1 First establish an Internet connection through either Dial-Up Networking or directly through a local area network (LAN) or wide area network (WAN).

From the Windows desktop system tray:

- 2 Verify the MUVPN client status—it must be activated. If it is not, right-click on the icon and select **Activate Security Policy**.

Then, from the Windows desktop:

- 3 Select **Start** ⇒ **Programs** ⇒ **Mobile User VPN** ⇒ **Connect**.
The WatchGuard Mobile User Connect window appears.
- 4 Click the **Yes** button.

The Mobile User VPN Client Icon

The Mobile User VPN icon exists in the Windows desktop system tray and displays several different status images. The following lists these images and provides a brief description of each:

Deactivated



The MUVPN Security Policy has been deactivated or the Windows operating system did not start a necessary Mobile User VPN service properly and the remote host computer must be restarted (if this continues you may need to reinstall the MUVPN client).

Activated



The MUVPN client is ready to establish a secure, VPN tunnel connection.

Activated and Transmitting Unsecured Data

The MUVPN client is ready to establish a secure, VPN tunnel connection and the red bar on the right of the icon indicates that the client has begun transmitting unsecured data.

Activated and Connected

The MUVPN client has established at least one secure, VPN tunnel connection but is not transmitting data.

Activated, Connected and Transmitting Unsecured Data

The MUVPN client has established at least one secure, VPN tunnel connection and the red bar on the right of the icon indicates that the client is transmitting only unsecured data.

Activated, Connected and Transmitting Secured Data

The MUVPN client has established at least one secure, VPN tunnel connection and the green bar on the right of the icon indicates that the client is transmitting only secured data.

Activated, Connected and Transmitting both Secure and Unsecured Data

The MUVPN client has established at least one secure, VPN tunnel connection and the red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

With the ZoneAlarm Firewall

The ZoneAlarm personal firewall will detect the attempt of the Mobile User Connect application to access the Internet. You must allow a couple of programs associated with this application access to the internet in order to establish the VPN tunnel.

The New Program alert dialog box appears requesting access for the MuvpnConnect.exe program.

From the ZoneAlarm alert dialog box:

- 1 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This will enable ZoneAlarm to allow the MuvpnConnect.exe program through each time you attempt to make a MUVPN connection.

The New Program alert dialog box appears requesting access for the IreIKE.exe program.

- 2 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This will enable ZoneAlarm to allow the IreIKE.exe program through each time you attempt to make a MUVPN connection.

Disconnect Mobile User VPN

The MUVPN tunnel is independent of the Internet connection. Close the MUVPN tunnels when the remote computer encounters either of the following events.

- Loses the Internet connection
- No longer needs the MUVPN tunnel

From the Windows desktop system tray:

- 1 Right-click on the Mobile User VPN Client icon.
- 2 Select **Disconnect All**.
The MUVPN Client closes all VPN tunnels. This process does not affect your connection to the Internet. You must disconnect from the Internet separately.
- 3 Right-click on the Mobile User VPN Client icon and select **Deactivate Security Policy**.
The MUVPN icon will display a red slash to indicate that the Security Policy has been deactivated.